RUHR UNIVERSITÄT BOCHUM

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Enrico Thomae

Präsenzübungen zur Vorlesung

Quantenalgorithmen

WS 2011/2012

Blatt 5 / 12 Dezember 2011

AUFGABE 1:
Sei $f : \mathbb{F}_2^n \to \mathbb{F}_2$. Gegeben ist ein Quanten-Schaltkreis Q_{n+1}, der für alle $x \in \mathbb{F}_2^n$, $y \in \mathbb{F}_2$ die lineare Abbildung $|xy\rangle \mapsto (-1)^{f(x)y}|xy\rangle$ berechnet. Konstruieren Sie unter Verwendung von Q_{n+1} einen Quantenschaltkreis, der die reversible Einbettung $U_f : |xy\rangle \mapsto |x\rangle \otimes |f(x) + y\rangle$ berechnet.

AUFGABE 2:
Sei $f(x_1, x_2, x_3, x_4) := (x_1 + x_2, x_2 + x_3, x_3 + x_4, x_4 + x_1)$ eine $2 : 1$ Abbildung.

(a) Führen Sie den Quantenschaltkreis des Algorithmus von Simon auf f aus.

(b) Angenommen Sie messen $y_1 = (1, 1, 0, 0)$, $y_2 = (1, 0, 1, 0)$, $y_3 = (1, 0, 0, 1)$.
Berechnen Sie daraus s.

(c) Zeigen Sie, dass $n - 1$ Vektoren aus $\mathbb{F}_2^n$ mit Wahrscheinlichkeit

$$\prod_{i=0}^{n-2}(1 - 2^{i-n})$$

linear unabhängig über $\mathbb{F}_2$ sind. Mit welcher Wahrscheinlichkeit reicht Ihnen die Messung von 3 Vektoren, um s in (b) zu bestimmen?

AUFGABE 3:
Berechnen Sie,

$$\mathrm{QFT}_2\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) \text{ und } \mathrm{QFT}_2\left(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right).$$